abgewichen, SOLLTE das mit dem oder der ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse SOLLTEN geeignet dokumentiert werden.

NET.3.1.A11 Beschaffung eines Routers oder Switches (S)

Bevor Router oder Switches beschafft werden, SOLLTE basierend auf der Sicherheitsrichtlinie eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es SOLLTE darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit den zu beschaffenden Geräten erreicht werden kann. Grundlage für die Beschaffung SOLLTEN daher die Anforderungen aus der Sicherheitsrichtlinie sein.

NET.3.1.A12 Erstellung einer Konfigurations-Checkliste für Router und Switches (S)

Es SOLLTE eine Konfigurations-Checkliste erstellt werden, anhand derer die wichtigsten sicherheitsrelevanten Einstellungen auf Routern und Switches geprüft werden können. Da die sichere Konfiguration stark vom Einsatzzweck abhängt, SOLLTEN die unterschiedlichen Anforderungen der Geräte in der Konfigurations-Checkliste berücksichtigt werden.

NET.3.1.A13 Administration über ein gesondertes Managementnetz (S)

Router und Switches SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert werden. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden.

NET.3.1.A14 Schutz vor Missbrauch von ICMP-Nachrichten (S)

Die Protokolle ICMP und ICMPv6 SOLLTEN restriktiv gefiltert werden.

NET.3.1.A15 Bogon- und Spoofing-Filterung (S)

Es SOLLTE verhindert werden, dass Angreifende mithilfe gefälschter, reservierter oder noch nicht zugewiesener IP-Adressen in die Router und Switches eindringen können.

NET.3.1.A16 Schutz vor „IPv6 Routing Header Type-0"-Angriffen (S)

Beim Einsatz von IPv6 SOLLTEN Mechanismen eingesetzt werden, die Angriffe auf den Routing-Header des Type-0 erkennen und verhindern.

NET.3.1.A17 Schutz vor DoS- und DDoS-Angriffen (S)

Es SOLLTEN Mechanismen eingesetzt werden, die hochvolumige Angriffe sowie TCP-State-Exhaustion-Angriffe erkennen und abwehren.

NET.3.1.A18 Einrichtung von Access Control Lists (S)

Der Zugriff auf Router und Switches SOLLTE mithilfe von Access Control Lists (ACLs) definiert werden. In der ACL SOLLTE anhand der Sicherheitsrichtlinie der Institution festgelegt werden, über welche IT-Systeme oder Netze mit welcher Methode auf einen Router oder Switch zugegriffen werden darf. Für den Fall, dass keine spezifischen Regeln existieren, SOLLTE generell der restriktivere Allowlist-Ansatz bevorzugt werden.

NET.3.1.A19 Sicherung von Switch-Ports (S)

Die Ports eines Switches SOLLTEN vor unberechtigten Zugriffen geschützt werden.

NET.3.1.A20 Sicherheitsaspekte von Routing-Protokollen (S)

Router SOLLTEN sich authentisieren, wenn sie Routing-Informationen austauschen oder Updates für Routing-Tabellen verschicken. Es SOLLTEN ausschließlich Routing-Protokolle eingesetzt werden, die dies unterstützen.

Dynamische Routing-Protokolle SOLLTEN ausschließlich in sicheren Netzen verwendet werden. Sie DÜRFEN NICHT in demilitarisierten Zonen (DMZs) eingesetzt werden. In DMZs SOLLTEN stattdessen statische Routen eingetragen werden.

NET.3.1.A21 Identitäts- und Berechtigungsmanagement in der Netzinfrastruktur (S)

Router und Switches SOLLTEN an ein zentrales Identitäts- und Berechtigungsmanagement angebunden werden.

NET.3.1.A22 Notfallvorsorge bei Routern und Switches (S)

Es SOLLTE geplant und vorbereitet werden, welche Fehler bei Routern oder Switches in einem Notfall diagnostiziert werden könnten. Außerdem SOLLTE geplant und vorbereitet werden, wie die identifizierten Fehler behoben werden können. Für typische Ausfallszenarien SOLLTEN entsprechende Handlungsanweisungen definiert und in regelmäßigen Abständen aktualisiert werden.

Die Notfallplanungen für Router und Switches SOLLTEN mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt sein. Die Notfallplanungen SOLLTEN sich am allgemeinen Notfallvorsorgekonzept orientieren. Es SOLLTE sichergestellt sein, dass die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform vorliegen. Das im Rahmen der Notfallvorsorge beschriebene Vorgehen SOLLTE regelmäßig geprobt werden.

NET.3.1.A23 Revision und Penetrationstests (S)

Router und Switches SOLLTEN regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Auch SOLLTEN regelmäßig Revisionen durchgeführt werden. Dabei SOLLTE unter anderem geprüft werden, ob der Ist-Zustand der festgelegten sicheren Grundkonfiguration entspricht. Die Ergebnisse SOLLTEN nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen SOLLTE nachgegangen werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.1.A24 Einsatz von Netzzugangskontrollen (H)

Eine Port-based Access Control SOLLTE nach IEEE 802.1x auf Basis von EAP-TLS implementiert werden. Es SOLLTE KEINE Implementierung nach den Standards IEEE 802.1x-2001 und IEEE 802.1x-2004 erfolgen.

NET.3.1.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (H)

Stürzt ein Router oder Switch ab, SOLLTE sichergestellt werden, dass bei der Wiederherstellung bzw. beim Neustart keine alten oder fehlerhaften Konfigurationen (unter anderem ACLs) benutzt werden.

NET.3.1.A26 Hochverfügbarkeit (H)

Die Realisierung einer Hochverfügbarkeitslösung SOLLTE den Betrieb der Router und Switches bzw. deren Sicherheitsfunktionen NICHT behindern oder das Sicherheitsniveau senken. Router und Switches SOLLTEN redundant ausgelegt werden. Dabei SOLLTE darauf geachtet werden, dass die Sicherheitsrichtlinie der Institution eingehalten wird.

NET.3.1.A27 Bandbreitenmanagement für kritische Anwendungen und Dienste (H)

Router und Switches SOLLTEN Funktionen enthalten und einsetzen, mit denen sich die Applikationen erkennen und Bandbreiten priorisieren lassen.

NET.3.1.A28 Einsatz von zertifizierten Produkten (H)

Es SOLLTEN Router und Switches mit einer Sicherheitsevaluierung nach Common Criteria eingesetzt werden, mindestens mit der Stufe EAL4.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den BSI-Standards zur Internet-Sicherheit (ISi-Reihe) weitere Informationen zur Sicherheit bei Routern und Switches veröffentlicht.

Das Institute of Electrical and Electronics Engineers (IEEE) hat in seiner Standard-Reihe die Standards IEEE 802.1Q „IEEE Standard for Local and Metropolitan Area Networks – Bridges and Bridged Networks“ und IEEE 802.1AE „IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security“ veröffentlicht.

In den Requests for Comments (RFC) bieten der RFC 6165 „Extensions to IS-IS for Layer-2 Systems“ und der RFC 7348 „Virtual Extensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks“ weiterführende Informationen zu Routern und Switches.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.2 Firewall

1. Beschreibung

1.1. Einleitung

Eine Firewall ist ein System aus soft- und hardwaretechnischen Komponenten, das dazu eingesetzt wird, IP-basierte Datennetze sicher zu koppeln. Dazu wird mithilfe einer Firewall-Struktur der technisch mögliche Informationsfluss auf die in einer Sicherheitsrichtlinie als vorher sicher definierte Kommunikation eingeschränkt. Sicher bedeutet hierbei, dass ausschließlich die erwünschten Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen werden.

Um Netzübergänge abzusichern, wird oft nicht mehr eine einzelne Komponente verwendet, sondern eine ganze Reihe von IT-Systemen, die unterschiedliche Aufgaben übernehmen, z. B. ausschließlich Pakete zu filtern oder Netzverbindungen mithilfe von Proxy-Funktionen strikt zu trennen. Der in diesem Baustein verwendete Begriff „Application Level Gateway" (ALG) bezeichnet eine Firewall-Komponente, die Datenströme auf Basis von Sicherheitsproxies regelt.

Eine Firewall wird am Übergang zwischen unterschiedlich vertrauenswürdigen Netzen eingesetzt. Unterschiedlich vertrauenswürdige Netze stellen dabei nicht unbedingt nur die Kombination aus Internet und Intranet dar. Vielmehr können auch zwei institutionsinterne Netze einen unterschiedlich hohen Schutzbedarf besitzen. So hat z. B. das Netz der Bürokommunikation meistens einen geringeren Schutzbedarf als das Netz der Personalabteilung, in dem besonders schützenswerte, personenbezogene Daten übertragen werden.

1.2. Zielsetzung

Ziel des Bausteins ist es, eine Firewall bzw. eine Firewall-Struktur mithilfe der in den folgenden Kapiteln beschriebenen Anforderungen sicher einsetzen zu können, um Netze mit unterschiedlichen Schutzanforderungen sicher miteinander zu verbinden.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.2 *Firewall* ist auf jede im Informationsverbund eingesetzte Firewall anzuwenden.

Ein typischer Anwendungsfall ist die Absicherung einer Außenverbindung, z. B. beim Übergang eines internen Netzes zum Internet oder bei Anbindungen zu Netzen von Partnerinstitutionen. Aber auch bei einer Kopplung von zwei institutionsinternen Netzen mit unterschiedlich hohem Schutzbedarf ist der Baustein anzuwenden, z. B. bei der Trennung des Bürokommunikationsnetzes vom Netz der Entwicklungsabteilung, wenn dort besonders vertrauliche Daten verarbeitet werden.

Der vorliegende Baustein baut auf den Baustein NET.1.1 *Netz-Architektur und -design* auf und enthält konkrete Anforderungen, die zu beachten und zu erfüllen sind, wenn netzbasierte Firewalls beschafft, aufgebaut, konfiguriert und betrieben werden.

Um Netze abzusichern, sind meistens weitere Netzkomponenten erforderlich, z. B. Router und Switches. Anforderungen hierzu werden jedoch nicht in diesem Baustein aufgeführt, sondern sind in NET.3.1 *Router und Switches* zu finden. Wenn eine Firewall die Aufgaben eines Routers oder Switches übernimmt, gelten für sie zusätzlich die Anforderungen des Bausteins NET.3.1 *Router und Switches*.

Darüber hinaus wird nicht auf Produkte wie sogenannte Next Generation Firewalls (NGFW) oder Unified Threat Management (UTM)-Firewalls eingegangen, die zusätzlich funktionale Erweiterungen enthalten, z. B. VPN, Systeme zur Intrusion Detection und Intrusion Prevention (IDS/IPS), Virenscanner oder Spam-Filter. Sicherheitsaspekte

dieser funktionalen Erweiterungen sind nicht Gegenstand des vorliegenden Bausteins, sondern werden z. B. in den Bausteinen NET.3.3 *VPN* und OPS1.1.4 *Schutz vor Schadprogrammen* behandelt.

Ebenso wird nicht auf eine Anwendungserkennung bzw. -filterung eingegangen. Sie ist eine gängige Funktion von Next Generation Firewalls sowie IDS/IPS. Da sich die Implementierungen zwischen den Produkten unterscheiden, wird empfohlen, sie je nach Einsatzszenario individuell zu betrachten. In diesem Baustein wird auch nicht auf die individuellen Schutzmöglichkeiten für extern angebotene Server-Dienste eingegangen, z. B. durch ein Reverse Proxy oder für Webdienste mithilfe einer Web Application Firewall (WAF). Darüber hinaus werden Aspekte der infrastrukturellen Sicherheit (z. B. geeignete Aufstellung oder Stromversorgung) nicht in diesem Baustein aufgeführt, sondern finden sich in den jeweiligen Bausteinen der Schicht INF *Infrastruktur*.

Firewalls sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.2 *Firewall* von besonderer Bedeutung.

2.1. Distributed Denial of Service (DDoS)

Bei einem DDoS-Angriff auf ein geschütztes Netz (z. B. TCP SYN Flooding, UDP Packet Storm) kann die Firewall aufgrund der vielen Netzverbindungen, die verarbeitet werden müssen, ausfallen. Das kann dazu führen, dass bestimmte Dienste im Local Area Network (LAN) nicht mehr verfügbar sind oder das gesamte LAN ausfällt.

2.2. Manipulation

Gelingt es Angreifenden, unberechtigt auf eine Firewall oder eine entsprechende Verwaltungsoberfläche zuzugreifen, können sie dort Dateien beliebig manipulieren. So können sie beispielsweise die Konfiguration ändern, zusätzliche Dienste starten oder Schadsoftware installieren. Ebenso können sie auf dem manipulierten IT-System die Kommunikationsverbindungen mitschneiden. Auch lassen sich beispielsweise die Firewall-Regeln so verändern, dass aus dem Internet auf die Firewall und auf das Intranet der Institution zugegriffen werden kann. Weiterhin können Angreifende einen Denial-of-Service (DoS)-Angriff starten, indem sie im Regelwerk den Zugriff auf einzelne Server-Dienste verhindern.

2.3. Umgehung der Firewall-Regeln

Angreifende können mithilfe grundlegender Mechanismen in den Netzprotokollen die Firewall-Regeln umgehen (z. B. durch Fragmentierungsangriffe), um in einen durch die Firewall geschützten Bereich einzudringen. Im geschützten Bereich können sie anschließend weiteren Schaden anrichten, z. B. schützenswerte Daten auslesen, manipulieren oder löschen.

2.4. Fehlerhafte Konfiguration und Bedienungsfehler einer Firewall

Eine fehlerhaft konfigurierte oder falsch bediente Firewall kann sich gravierend auf die Verfügbarkeit von Diensten auswirken. Werden beispielsweise Firewall-Regeln falsch gesetzt, können Netzzugriffe blockiert werden. Weiterhin können fehlerhafte Konfigurationen dazu führen, dass IT-Systeme nicht mehr vollständig oder gar nicht mehr geschützt sind. Im schlimmsten Fall sind dadurch interne Dienste für Angreifende erreichbar.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.2 *Firewall* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.2.A1 Erstellung einer Sicherheitsrichtlinie (B)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie erstellt werden. In dieser MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie Firewalls sicher betrieben werden können. Die Richtlinie MUSS allen im Bereich Firewalls zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Die Ergebnisse MÜSSEN sinnvoll dokumentiert werden.

NET.3.2.A2 Festlegen der Firewall-Regeln (B)

Die gesamte Kommunikation zwischen den beteiligten Netzen MUSS über die Firewall geleitet werden. Es MUSS sichergestellt sein, dass von außen keine unerlaubten Verbindungen in das geschützte Netz aufgebaut werden können. Ebenso DÜRFEN KEINE unerlaubten Verbindungen aus dem geschützten Netz heraus aufgebaut werden.

Für die Firewall MÜSSEN eindeutige Regeln definiert werden, die festlegen, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen MÜSSEN durch die Firewall unterbunden werden (Allowlist-Ansatz). Die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern, die über die Firewall geführt werden, MÜSSEN in den Regeln berücksichtigt sein.

Es MÜSSEN Zuständige benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem MUSS geklärt werden, wer Filterregeln verändern darf. Die getroffenen Entscheidungen sowie die relevanten Informationen und Entscheidungsgründe MÜSSEN dokumentiert werden.

NET.3.2.A3 Einrichten geeigneter Filterregeln am Paketfilter (B)

Basierend auf den Firewall-Regeln aus NET.3.2.A2 *Festlegen der Firewall-Regeln* MÜSSEN geeignete Filterregeln für den Paketfilter definiert und eingerichtet werden.

Ein Paketfilter MUSS so eingestellt sein, dass er alle ungültigen TCP-Flag-Kombinationen verwirft. Grundsätzlich MUSS immer zustandsbehaftet gefiltert werden. Auch für die verbindungslosen Protokolle UDP und ICMP MÜSSEN zustandsbehaftete Filterregeln konfiguriert werden. Die Firewall MUSS die Protokolle ICMP und ICMPv6 restriktiv filtern.

NET.3.2.A4 Sichere Konfiguration der Firewall (B)

Bevor eine Firewall eingesetzt wird, MUSS sie sicher konfiguriert werden. Alle Konfigurationsänderungen MÜSSEN nachvollziehbar dokumentiert sein. Die Integrität der Konfigurationsdateien MUSS geeignet geschützt werden. Bevor Zugangspasswörter abgespeichert werden, MÜSSEN sie mithilfe eines zeitgemäßen kryptografischen Verfahrens abgesichert werden (siehe CON.1 *Kryptokonzept*). Eine Firewall MUSS so konfiguriert sein, dass ausschließlich zwingend erforderliche Dienste verfügbar sind. Wenn funktionale Erweiterungen benutzt werden, MÜSSEN die Sicherheitsrichtlinien der Institution weiterhin erfüllt sein. Auch MUSS begründet und dokumentiert werden, warum solche Erweiterungen eingesetzt werden. Nicht benötigte (Auskunfts-)Dienste sowie nicht benötigte funktionale Erweiterungen MÜSSEN deaktiviert oder ganz deinstalliert werden. Informationen über den internen Konfigurations- und Betriebszustand MÜSSEN nach außen bestmöglich verborgen werden.

NET.3.2.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A6 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Managementzugänge der Firewall MÜSSEN auf einzelne Quell-IP-Adressen bzw. -Adressbereiche eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Firewall zu administrieren bzw. zu überwachen, DÜRFEN NUR sichere Protokolle eingesetzt werden. Alternativ MUSS ein eigens dafür vorgesehenes Administrationsnetz (Out-of-Band-Management) verwendet werden. Für die Bedienschnittstellen MÜSSEN geeignete Zeitbeschränkungen vorgegeben werden.

NET.3.2.A7 Notfallzugriff auf die Firewall (B)

Es MUSS immer möglich sein, direkt auf die Firewall zugreifen zu können, sodass sie im Notfall auch dann lokal administriert werden kann, wenn das gesamte Netz ausfällt.

NET.3.2.A8 Unterbindung von dynamischem Routing (B)

In den Einstellungen der Firewall MUSS das dynamische Routing deaktiviert sein, es sei denn, der Paketfilter wird entsprechend dem Baustein NET.3.1 *Router und Switches* als Perimeter-Router eingesetzt.

NET.3.2.A9 Protokollierung (B)

Die Firewall MUSS so konfiguriert werden, dass sie mindestens folgende sicherheitsrelevante Ereignisse protokolliert:

- abgewiesene Netzverbindungen (Quell- und Ziel-IP-Adressen, Quell- und Zielport oder ICMP/ICMPv6-Typ, Datum, Uhrzeit),
- fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen,
- Fehlermeldungen der Firewall-Dienste,
- allgemeine Systemfehlermeldungen und
- Konfigurationsänderungen (möglichst automatisch).

Werden Sicherheitsproxies eingesetzt, MÜSSEN Sicherheitsverletzungen und Verstöße gegen Access-Control-Listen (ACLs oder auch kurz Access-Listen) in geeigneter Weise protokolliert werden. Hierbei MÜSSEN mindestens die Art der Protokollverletzung bzw. des ACL-Verstoßes, Quell- und Ziel-IP-Adresse, Quell- und Zielport, Dienst, Datum und Zeit sowie, falls erforderlich, die Verbindungsdauer protokolliert werden.

Wenn sich Benutzende am Sicherheitsproxy authentisieren, MÜSSEN auch Authentisierungsdaten oder ausschließlich die Information über eine fehlgeschlagene Authentisierung protokolliert werden.

NET.3.2.A10 Abwehr von Fragmentierungsangriffen am Paketfilter (B)

Am Paketfilter MÜSSEN Schutzmechanismen aktiviert sein, um IPv4- sowie IPv6 Fragmentierungsangriffe abzuwehren.

NET.3.2.A11 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A12 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A13 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.3.2.A14 Betriebsdokumentationen (B)

Die betrieblichen Aufgaben einer Firewall MÜSSEN nachvollziehbar dokumentiert werden. Es MÜSSEN alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben dokumentiert werden, insbesondere Änderungen an den Systemdiensten und dem Regelwerk der Firewall. Die Dokumentation MUSS vor unbefugten Zugriffen geschützt werden.

NET.3.2.A15 Beschaffung einer Firewall (B)

Bevor eine Firewall beschafft wird, MUSS eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden. Es MUSS darauf geachtet werden, dass das von der Institution angestrebte Sicherheitsniveau mit der Firewall erreichbar ist. Grundlage für die Beschaffung MÜSSEN daher die Anforderungen aus der Sicherheitsrichtlinie sein.

Wird IPv6 eingesetzt, MUSS der Paketfilter die IPv6-Erweiterungsheader (Extension Header) überprüfen. Zudem MUSS sich IPv6 adäquat zu IPv4 konfigurieren lassen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.2.A16 Aufbau einer „P-A-P"-Struktur (S)

Eine „Paketfilter – Application-Level-Gateway – Paketfilter"-(P-A-P)-Struktur SOLLTE eingesetzt werden. Sie MUSS aus mehreren Komponenten mit jeweils dafür geeigneter Hard- und Software bestehen. Für die wichtigsten verwendeten Protokolle SOLLTEN Sicherheitsproxies auf Anwendungsschicht vorhanden sein. Für andere Dienste SOLLTEN zumindest generische Sicherheitsproxies für TCP und UDP genutzt werden. Die Sicherheitsproxies SOLLTEN zudem innerhalb einer abgesicherten Laufzeitumgebung des Betriebssystems ablaufen.

NET.3.2.A17 Deaktivierung von IPv4 oder IPv6 (S)

Wenn das IPv4- oder IPv6-Protokoll in einem Netzsegment nicht benötigt wird, SOLLTE es am jeweiligen Firewall-Netzzugangspunkt (z. B. am entsprechenden Firewall-Interface) deaktiviert werden. Falls das IPv4- oder IPv6-Protokoll nicht benötigt bzw. eingesetzt wird, SOLLTE es auf der Firewall komplett deaktiviert werden.

NET.3.2.A18 Administration über ein gesondertes Managementnetz (S)

Firewalls SOLLTEN ausschließlich über ein separates Managementnetz (Out-of-Band-Management) administriert werden. Eine eventuell vorhandene Administrationsschnittstelle über das eigentliche Datennetz (In-Band) SOLLTE deaktiviert werden. Die Kommunikation im Managementnetz SOLLTE über Management-Firewalls (siehe NET.1.1 *Netz-Architektur und -design*) auf wenige Managementprotokolle mit genau festgelegten Ursprüngen und Zielen beschränkt werden. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert sein. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden (siehe NET.1.2 *Netzmanagement*).

NET.3.2.A19 Schutz vor TCP SYN Flooding, UDP Paket Storm und Sequence Number Guessing am Paketfilter (S)

Am Paketfilter, der Server-Dienste schützt, die aus nicht vertrauenswürdigen Netzen erreichbar sind, SOLLTE ein geeignetes Limit für halboffene und offene Verbindungen gesetzt werden.

Am Paketfilter, der Server-Dienste schützt, die aus weniger oder nicht vertrauenswürdigen Netzen erreichbar sind, SOLLTEN die sogenannten Rate Limits für UDP-Datenströme gesetzt werden.

Am äußeren Paketfilter SOLLTE bei ausgehenden Verbindungen für TCP eine zufällige Generierung von Initial Sequence Numbers (ISN) aktiviert werden, sofern dieses nicht bereits durch Sicherheitsproxies realisiert wird.

NET.3.2.A20 Absicherung von grundlegenden Internetprotokollen (S)

Die Protokolle HTTP, SMTP und DNS inklusive ihrer verschlüsselten Versionen SOLLTEN über protokollspezifische Sicherheitsproxies geleitet werden.

NET.3.2.A21 Temporäre Entschlüsselung des Datenverkehrs (S)

Verschlüsselte Verbindungen in nicht vertrauenswürdige Netze SOLLTEN temporär entschlüsselt werden, um das Protokoll zu verifizieren und die Daten auf Schadsoftware zu prüfen. Hierbei SOLLTEN die rechtlichen Rahmenbedingungen beachtet werden.

Die Komponente, die den Datenverkehr temporär entschlüsselt, SOLLTE unterbinden, dass veraltete Verschlüsselungsoptionen und kryptografische Algorithmen benutzt werden.

Der eingesetzte TLS-Proxy SOLLTE prüfen können, ob Zertifikate vertrauenswürdig sind. Ist ein Zertifikat nicht vertrauenswürdig, SOLLTE es möglich sein, die Verbindung abzuweisen. Eigene Zertifikate SOLLTEN nachrüstbar sein, um auch „interne" Root-Zertifikate konfigurieren und prüfen zu können. Vorkonfigurierte Zertifikate SOLLTEN überprüft und entfernt werden, wenn sie nicht benötigt werden.

NET.3.2.A22 Sichere Zeitsynchronisation (S)

Die Uhrzeit der Firewall SOLLTE mit einem Network-Time-Protocol (NTP)-Server synchronisiert werden. Die Firewall SOLLTE keine externe Zeitsynchronisation zulassen.

NET.3.2.A23 Systemüberwachung und -Auswertung (S)

Firewalls SOLLTEN in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Es SOLLTE ständig überwacht werden, ob die Firewall selbst sowie die darauf betriebenen Dienste korrekt funktionieren. Bei Fehlern oder wenn Grenzwerte überschritten werden, SOLLTE das Betriebspersonal alarmiert werden. Zudem SOLLTEN automatische Alarmmeldungen generiert werden, die bei festgelegten Ereignissen ausgelöst werden. Protokolldaten oder Statusmeldungen SOLLTEN nur über sichere Kommunikationswege übertragen werden.

NET.3.2.A24 Revision und Penetrationstests (S)

Die Firewall-Struktur SOLLTE regelmäßig auf bekannte Sicherheitsprobleme hin überprüft werden. Es SOLLTEN regelmäßige Penetrationstests und Revisionen durchgeführt werden.

NET.3.2.A32 Notfallvorsorge für die Firewall (S)

Diagnose und Fehlerbehebungen SOLLTEN bereits im Vorfeld geplant und vorbereitet werden. Für typische Ausfallszenarien SOLLTEN entsprechende Handlungsanweisungen definiert und in regelmäßigen Abständen aktualisiert werden.

Die Notfallplanungen für die Firewall SOLLTEN mit der übergreifenden Störungs- und Notfallvorsorge abgestimmt sein. Sie SOLLTEN sich am allgemeinen Notfallvorsorgekonzept orientieren (siehe DER.4 *Notfallmanagement*). Es SOLLTE sichergestellt sein, dass die Dokumentationen zur Notfallvorsorge und die darin enthaltenen Handlungsanweisungen in Papierform vorliegen. Das im Rahmen der Notfallvorsorge beschriebene Vorgehen SOLLTE regelmäßig geprobt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.2.A25 Erweiterter Integritätsschutz für die Konfigurationsdateien (H)

Um eine abgestürzte Firewall wiederherzustellen, SOLLTE sichergestellt werden, dass keine alten oder fehlerhaften Konfigurationen (unter anderem Access-Listen) benutzt werden. Dies SOLLTE auch gelten, wenn es bei einem Angriff gelingt, die Firewall neu zu starten.

NET.3.2.A26 Auslagerung von funktionalen Erweiterungen auf dedizierte Hardware (H)

Funktionale Erweiterungen der Firewall SOLLTEN auf dedizierte Hard- und Software ausgelagert werden.

NET.3.2.A27 Einsatz verschiedener Firewall-Betriebssysteme und -Produkte in einer mehrstufigen Firewall-Architektur (H)

In einer mehrstufigen Firewall-Architektur SOLLTEN unterschiedliche Betriebssysteme und -Produkte für die äußeren und inneren Firewalls eingesetzt werden.

NET.3.2.A28 Zentrale Filterung von aktiven Inhalten (H)

Aktive Inhalte SOLLTEN gemäß den Sicherheitszielen der Institution zentral gefiltert werden. Dafür SOLLTE auch der verschlüsselte Datenverkehr entschlüsselt werden. Die erforderlichen Sicherheitsproxies SOLLTEN es unterstützen, aktive Inhalte zu filtern.

NET.3.2.A29 Einsatz von Hochverfügbarkeitslösungen (H)

Paketfilter und Application-Level-Gateway SOLLTEN hochverfügbar ausgelegt werden. Zudem SOLLTEN zwei voneinander unabhängige Zugangsmöglichkeiten zum externen Netz bestehen, z. B. zwei Internetzugänge von unterschiedlichen Providern. Interne und externe Router sowie alle weiteren beteiligten aktiven Komponenten (z. B. Switches) SOLLTEN ebenfalls hochverfügbar ausgelegt sein.

Auch nach einem automatischen Failover SOLLTE die Firewall-Struktur die Anforderungen der Sicherheitsrichtlinie erfüllen (Fail safe bzw. Fail secure).

Die Funktion SOLLTE anhand von zahlreichen Parametern überwacht werden. Die Funktionsüberwachung SOLLTE sich nicht auf ein einzelnes Kriterium stützen. Protokolldateien und Warnmeldungen der Hochverfügbarkeitslösung SOLLTEN regelmäßig kontrolliert werden.

NET.3.2.A30 Bandbreitenmanagement für kritische Anwendungen und Dienste (H)

Um Bandbreitenmanagement für kritische Anwendungen und Dienste zu gewährleisten, SOLLTEN Paketfilter mit entsprechender Bandbreitenmanagementfunktion an Netzübergängen und am Übergang zwischen verschiedenen Sicherheitszonen eingesetzt werden.

NET.3.2.A31 Einsatz von zertifizierten Produkten (H)

Firewalls mit einer Sicherheitsevaluierung nach Common Criteria SOLLTEN eingesetzt werden, mindestens mit der Stufe EAL4.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat folgende weiterführende Dokumente zum Themenfeld Firewall veröffentlicht:

- Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 – Version 2.0
- Kryptographische Verfahren: Empfehlungen und Schlüssellängen – Teil 2: Verwendung von Transport Layer Security (TLS): BSI-TR-02102-2
- Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-41 „Guidelines on Firewalls and Firewall Policy“ Empfehlungen zum Einsatz von Firewalls.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.3 VPN

1. Beschreibung

1.1. Einleitung

Mithilfe von Virtuellen Privaten Netzen (VPNs) können schutzbedürftige Daten über nicht-vertrauenswürdige Netze, wie das Internet, übertragen werden. Ein VPN ist ein virtuelles Netz, das innerhalb eines anderen Netzes betrieben wird, jedoch logisch von diesem Netz getrennt ist. Das VPN nutzt das Netz hierbei lediglich als Transportmedium, ist aber selber unabhängig von der Struktur und dem Aufbau des verwendeten Netzes. VPNs können mithilfe kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten schützen. VPNs ermöglichen auch dann die sichere Authentisierung der Kommunikationspunkte, wenn mehrere Netze oder IT-Systeme über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.

1.2. Zielsetzung

Der Baustein definiert Anforderungen, mit denen sich ein VPN zielgerichtet und sicher planen, umsetzen und betreiben lässt.

1.3. Abgrenzung und Modellierung

Der vorliegende Baustein ist für jede Zugriffsmöglichkeit auf das Netz der Institution über einen VPN-Endpunkt anzuwenden.

Der Baustein geht nicht auf Grundlagen für sichere Netze und deren Aufbau ein (siehe dazu NET.1.1 *Netzarchitektur und -design*). Auch deckt dieser Baustein nicht alle mit dem Betrieb eines VPN zusammenhängenden Prozesse ab. VPNs sollten grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.2.5 *Fernwartung*, OPS.1.1.2 *Ordnungsgemäße IT-Administration* sowie CON.1 *Kryptokonzept* mit berücksichtigt werden.

Empfehlungen, wie die Betriebssysteme der VPN-Endpunkte konfiguriert werden können, sind ebenfalls nicht Bestandteil dieses Bausteins. Entsprechende Anforderungen sind im Baustein SYS.1.1 *Allgemeiner Server* beziehungsweise SYS.2.1 *Allgemeiner Client* sowie in den jeweiligen betriebssystemspezifischen Bausteinen des IT-Grundschutz-Kompendiums zu finden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.3 *VPN* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung des VPN-Einsatzes

Bei einem nicht sorgfältig geplanten, aufgebauten oder konfigurierten VPN können Sicherheitslücken entstehen, die alle IT-Systeme betreffen könnten, die mit dem VPN verbunden sind. Angreifenden kann es so möglich sein, auf vertrauliche Informationen der Institution zuzugreifen.

So ist es durch eine unzureichende VPN-Planung beispielsweise möglich, dass die Benutzenden nicht ordnungsgemäß geschult wurden. Dadurch könnten sie das VPN in einer unsicheren Umgebung benutzen oder sich von unsicheren Clients aus einwählen. Dies ermöglicht es Angreifenden eventuell, auf das gesamte Institutionsnetz zuzugreifen.

Auch wenn die regelmäßige Kontrolle der Zugriffe auf das VPN unzureichend geplant wurde, könnten Angriffe nicht rechtzeitig erkannt werden. Somit kann nicht zeitnah reagiert werden und Angreifende unbemerkt Daten stehlen oder ganze Prozesse sabotieren.

2.2. Unsichere VPN-Dienstleistende

Hat eine Institution seine VPN-Dienstleistenden nicht sorgfältig ausgewählt, könnte dadurch das gesamte Netz der Institution unsicher werden. So könnte beispielsweise ein von den Dienstleistenden unsicher angebotener VPN-Zugang für Angriffe genutzt werden, um gezielt Informationen zu stehlen.

2.3. Unsichere Konfiguration der VPN-Clients für den Fernzugriff

Wird ein VPN-Client nicht sicher konfiguriert, könnten die Benutzenden dessen Sicherheitsmechanismen falsch oder gar nicht benutzen. Auch verändern sie eventuell die Konfiguration des VPN-Clients. Ebenso ist es durch eine unsichere Konfiguration möglich, dass von den Benutzenden installierte Software auch die Sicherheit des VPN-Clients gefährdet.

2.4. Unsichere Standard-Einstellungen auf VPN-Komponenten

In der Standard-Einstellung sind VPN-Komponenten meist ohne oder nur mit unzureichenden Sicherheitsmechanismen vorkonfiguriert. Oft wird mehr auf Nutzungsfreundlichkeit und problemlose Integration in bestehende IT-Systeme als auf Sicherheit geachtet. Werden VPN-Komponenten nicht oder nur mangelhaft an die konkreten Sicherheitsbedürfnisse der Institution angepasst, können Schwachstellen und somit gefährliche Angriffspunkte entstehen. Werden beispielsweise werksseitig voreingestellte Passwörter nicht geändert, könnte das gesamte VPN und damit das interne Netz der Institution angegriffen werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.3 *VPN* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.3.A1 Planung des VPN-Einsatzes (B)

Die Einführung eines VPN MUSS sorgfältig geplant werden. Dabei MÜSSEN die Verantwortlichkeiten für den VPN-Betrieb festgelegt werden. Es MÜSSEN für das VPN zudem Benutzendengruppen und deren Berechtigungen geplant werden. Ebenso MUSS definiert werden, wie erteilte, geänderte oder entzogene Zugriffsberechtigungen zu dokumentieren sind.

NET.3.3.A2 Auswahl von VPN-Dienstleistenden (B)

Falls VPN-Dienstleistende eingesetzt werden, MÜSSEN mit diesen Service Level Agreements (SLAs) ausgehandelt und schriftlich dokumentiert werden. Es MUSS regelmäßig kontrolliert werden, ob die VPN-Dienstleistenden die vereinbarten SLAs einhalten.

NET.3.3.A3 Sichere Installation von VPN-Endgeräten (B)

Wird eine Appliance eingesetzt, die eine Wartung benötigt, MUSS es dafür einen gültigen Wartungsvertrag geben. Es MUSS sichergestellt werden, dass nur qualifiziertes Personal VPN-Komponenten installiert. Die Installation der VPN-Komponenten sowie eventuelle Abweichungen von den Planungsvorgaben SOLLTEN dokumentiert werden. Die Funktionalität und die gewählten Sicherheitsmechanismen des VPN MÜSSEN vor Inbetriebnahme geprüft werden.

NET.3.3.A4 Sichere Konfiguration eines VPN (B)

Für alle VPN-Komponenten MUSS eine sichere Konfiguration festgelegt werden. Diese SOLLTE geeignet dokumentiert werden. Auch MUSS die für die Administration zuständige Person regelmäßig kontrollieren, ob die Konfiguration noch sicher ist und sie eventuell für alle IT-Systeme anpassen.

NET.3.3.A5 Sperrung nicht mehr benötigter VPN-Zugänge (B)

Es MUSS regelmäßig geprüft werden, ob ausschließlich berechtigte IT-Systeme und Benutzende auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge MÜSSEN zeitnah deaktiviert werden. Der VPN-Zugriff MUSS auf die benötigten Benutzungszeiten beschränkt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.3.A6 Durchführung einer VPN-Anforderungsanalyse (S)

Eine Anforderungsanalyse SOLLTE durchgeführt werden, um für das jeweilige VPN die Einsatzszenarien zu bestimmen und daraus Anforderungen an die benötigten Hard- und Software-Komponenten ableiten zu können. In der Anforderungsanalyse SOLLTEN folgende Punkte betrachtet werden:

- Geschäftsprozesse beziehungsweise Fachaufgaben,
- Zugriffswege,
- Identifikations- und Authentisierungsverfahren,
- Benutzende und ihre Berechtigungen,
- Zuständigkeiten sowie
- Meldewege.

NET.3.3.A7 Planung der technischen VPN-Realisierung (S)

Neben der allgemeinen Planung (siehe NET.3.3.A1 *Planung des VPN-Einsatzes*) SOLLTEN die technischen Aspekte eines VPN sorgfältig geplant werden. So SOLLTEN für das VPN die Verschlüsselungsverfahren, VPN-Endpunkte, erlaubten Zugangsprotokolle, Dienste und Ressourcen festgelegt werden. Zudem SOLLTEN die Teilnetze definiert werden, die über das VPN erreichbar sind. (siehe NET.1.1 *Netzarchitektur und -design).*

NET.3.3.A8 Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung (S)

Eine Sicherheitsrichtlinie zur VPN-Nutzung SOLLTE erstellt werden. Diese SOLLTE allen Mitarbeitenden bekannt gegeben werden. Die in der Sicherheitsrichtlinie beschriebenen Sicherheitsmaßnahmen SOLLTEN im Rahmen von Schulungen erläutert werden. Wird für Mitarbeitende ein VPN-Zugang eingerichtet, SOLLTE diesen ein Merkblatt mit den wichtigsten VPN-Sicherheitsmechanismen ausgehändigt werden. Alle VPN-Benutzende SOLLTEN verpflichtet werden, die Sicherheitsrichtlinien einzuhalten.

NET.3.3.A9 Geeignete Auswahl von VPN-Produkten (S)

Bei der Auswahl von VPN-Produkten SOLLTEN die Anforderungen der Institutionen an die Vernetzung unterschiedlicher Standorte und die Anbindung von mobilen Mitarbeitenden oder Telearbeitsplätzen berücksichtigt werden.

NET.3.3.A10 Sicherer Betrieb eines VPN (S)

Für VPNs SOLLTE ein Betriebskonzept erstellt werden. Darin SOLLTEN die Aspekte Qualitätsmanagement, Überwachung, Wartung, Schulung und Autorisierung beachtet werden.

NET.3.3.A11 Sichere Anbindung eines externen Netzes (S)

Es SOLLTE sichergestellt werden, dass VPN-Verbindungen NUR zwischen den dafür vorgesehenen IT-Systemen und Diensten aufgebaut werden. Die dabei eingesetzten Tunnel-Protokolle SOLLTEN für den Einsatz geeignet sein.

NET.3.3.A12 Konten- und Zugriffsverwaltung bei Fernzugriff-VPNs (S)

Für Fernzugriff-VPNs SOLLTE eine zentrale und konsistente Konten- und Zugriffsverwaltung gewährleistet werden.

NET.3.3.A13 Integration von VPN-Komponenten in eine Firewall (S)

Die VPN-Komponenten SOLLTEN in die Firewall integriert werden. Dies SOLLTE dokumentiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27033-5:2013 „Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“ Vorgaben für den Einsatz von VPNs.

Das National Institute of Standards and Technology (NIST) macht in seiner Special Publication 800-77 „Guide to IPsec VPNs“ generelle Vorgaben zum Einsatz von VPNs.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.3.4 Network Access Control

1. Beschreibung

1.1. Einleitung

Eine Netzzugangskontrolle (engl. Network Access Control, NAC) sichert Netzzugänge im Endgerätebereich durch Identitätsprüfung (Authentisierung) und Reglementierung (Autorisierung) ab. Unter Endgeräten werden in diesem Baustein alle IT-Systeme verstanden, die am Access Layer eines Campus-Netzes angeschlossen werden. NAC kann sowohl in kabelgebundenen als auch in drahtlosen Netzen eingesetzt werden. Eine Identität kann zum Beispiel über Konten mit Zertifikaten sicher geprüft werden. Durch die folgende Autorisierung werden den Endgeräten über Autorisierungsregeln passende Netzsegmente und Berechtigungen zugewiesen und damit Zugriffsregeln festgelegt. Ebenso kann Endgeräten der Netzzugang verweigert werden.

Beispielsweise kann ein Drucker über NAC als solcher identifiziert und mit einem validen Zertifikat sicher authentisiert werden. Wurde der Drucker erfolgreich authentisiert, wird er dann mittels NAC-Autorisierung dem für den Drucker vorgesehenen Netzsegment zugewiesen.

NAC-Lösungen nutzen dabei entweder die im Standard IEEE 802.1X (Port Based Network Access Control) beschriebenen Techniken oder die sogenannte MAC-Adress-Authentisierung. Bei IEEE 802.1X erfolgt die Authentisierung über das Extensible Authentication Protocol (EAP) zwischen einer Software auf dem Endgerät, dem sogenannten Supplicant, und dem sogenannten Authenticator, der von einem Access-Switch, WLAN Access Point oder WLAN Controller realisiert wird. Für die Authentisierung wird zusätzlich ein zentraler RADIUS-Server (Remote Authentication Dial-In User Service) genutzt. Der RADIUS-Server wird auch als Authentication Server oder AAA-Server (Authentication, Authorization, Accounting) bezeichnet. Bei der MAC-Adress-Authentisierung wird das Endgerät über seine MAC-Adresse authentisiert.

Eine NAC-Lösung nach IEEE 802.1X umfasst also folgende Komponenten:

- Authentication Server oder RADIUS-Server
- Supplicant auf einem Endgerät
- Authenticator auf einem Access-Switch oder einer WLAN-Komponente (WLAN Access Point oder WLAN Controller)
- zentrale NAC-Identitätsverwaltung, die als integrierte Identitätsverwaltung auf dem Server realisiert sein kann oder auf bestehende Verzeichnisdienste zurückgreift

Eine NAC-Lösung umfasst in diesem Baustein alle zuvor beschriebenen Komponenten. Ist eine einzelne Komponente der NAC-Lösung gemeint, z. B. der RADIUS-Server, dann wird diese Komponente tatsächlich auch als solche benannt. Als zentrale Komponenten einer NAC-Lösung gelten in diesem Baustein der RADIUS-Server und die NAC-Identitätsverwaltung.

Damit eine NAC-Lösung sinnvoll eingesetzt werden kann und die Netzzugänge geeignet abgesichert werden können, müssen viele Punkte festgelegt und die genannten Komponenten der Lösung aufeinander abgestimmt werden. Weiterhin sind NAC-spezifische Prozesse (z. B. Maßnahmen, um Störungen zu beheben) zu definieren und bestehende Prozesse (z. B. Inbetriebnahme von Endgeräten) anzupassen.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei NAC zu etablieren. Eine NAC-Lösung soll sicherstellen, dass der Zugang zum Netz durch identitätsabhängige Autorisierungsregeln reglementiert wird. Dadurch werden Informationen geschützt, die über Netze verarbeitet, gespeichert und übertragen werden.

1.3. Abgrenzung und Modellierung

Der Baustein NET.3.4 *Network Access Control* ist auf die Elemente einer NAC-Lösung anzuwenden. Dies beinhaltet betroffene Netze, Clients und zentrale Komponenten.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt NAC-Lösungen, die auf dem Standard IEEE 802.1X und MAC-Adress-Authentisierung via RADIUS basieren. Dabei liegt der Fokus auf folgende Teilaspekte einer NAC-Lösung:

- allgemeine Festlegungen für NAC sowohl für die zentralen Komponenten als auch für die Endgeräte
- Anforderungen an Authentisierung und Autorisierung
- Festlegungen für Management und Betrieb einer NAC-Lösung

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Verzeichnisdienste (siehe APP.2.1 *Allgemeiner Verzeichnisdienst*)
- Netzarchitektur und -design (siehe NET.1.1 *Netzarchitektur und -design*)
- WLAN-spezifische Aspekte (siehe NET.2.1 *WLAN-Betrieb* und NET.2.2 *WLAN-Nutzung*)
- allgemeine Betriebsaspekte (siehe Bausteine der Schicht OPS *Betrieb*)

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Port Security sowie allgemeine Aspekte für Netzkomponenten (siehe NET.3.1 *Router und Switches*)
- proprietäre NAC-Implementierungen, die nicht auf IEEE 802.1X basieren
- die Implementierung eines RADIUS-Servers auf Netzkomponenten (Access-Switch, WLAN Access Point oder WLAN Controller)
- administrative Authentisierung an Netzkomponenten mittels RADIUS
- allgemeine Aspekte für Endgeräte (siehe Bausteine der Schichten SYS.2 *Desktop-Systeme*, SYS.3 *Mobile Devices* und SYS.4 *Sonstige Systeme*)
- allgemeine Aspekte für Server (siehe SYS.1.1 *Allgemeiner Server*) und Virtualisierung (siehe SYS.1.5 *Virtualisierung*)
- allgemeine Aspekte für Identitäts- und Berechtigungsmanagement (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.3.4 *Network Access Control* von besonderer Bedeutung.

2.1. Unzureichende Planung der NAC-Lösung

Sind nicht alle für NAC relevanten IT-Systeme und Informationen in einem IT-Asset-Management erfasst, kann eine NAC-Lösung nicht ausreichend geplant werden. Endgeräte erhalten dann gegebenenfalls keinen Zugang zum Netz oder einen Zugang zu einem falschen Netzsegment.

Wurden die Anforderungen an die NAC-Lösung nicht ausreichend erfasst und analysiert, kann auch dies zu einer unzureichenden Planung führen. Beispielsweise ist es dann möglich, dass eingesetzte Switches die Anforderungen an die geplante NAC-Lösung nicht erfüllen können oder der geplante RADIUS-Server falsch dimensioniert wird. Eine weitere Folge könnten auch zu harte oder zu weiche Vorgaben für die genutzten Authentisierungs- und Autorisierungsverfahren sein. Dadurch könnte Endgeräten entweder der Zugang zum Netz verweigert oder unsichere Authentisierungsverfahren könnten genutzt werden, obwohl sichere Verfahren möglich wären. Möglicherweise könnten dadurch auch zu weitreichende Kommunikationsberechtigungen erlangt werden.

2.2. Unzureichend abgestimmte Integration von Endgeräten in die NAC-Lösung

Fehlende oder unzureichend umgesetzte Orchestrierungswerkzeuge, Sicherheitsrichtlinien, Anforderungskataloge und Ressourcen für die Erfassung aller Endgeräte können dazu führen, dass Endgeräte unzureichend abgestimmt in die NAC-Lösung integriert werden. Dies erschwert es, ein sicheres und betriebsfreundliches Authentisierungsverfahren je Endgerätegruppe umzusetzen und ein entsprechendes Inbetriebnahmeverfahren zu konzipieren. Dadurch könnten die Kommunikationsmöglichkeiten der Endgeräte negativ beeinträchtigt werden. Außerdem kann es sein, dass zu schützende Geräte versehentlich in falschen Netzsegmenten positioniert werden.

Sind die Endgeräte unzureichend standardisiert oder werden NAC-spezifische Endgeräteanforderungen unzureichend unterstützt, kann dies auch dazu führen, dass unsichere Authentisierungsverfahren eingesetzt werden, obwohl eine starke Authentisierung grundsätzlich möglich wäre.

2.3. Nutzung unzureichend sicherer Protokolle bei NAC

Werden sichere EAP-Authentisierungsverfahren technisch nicht unterstützt, kann es passieren, dass unsichere Authentisierungsprotokolle wie EAP-MD5 oder MAC-Authentisierung eingesetzt werden müssen. In diesem Fall sind Spoofing-, Replay- oder Man-in-the-Middle-Angriffe leichter möglich und es kann nicht ausgeschlossen werden, dass unberechtigte IT-Systeme in das Netz gelangen. Wird für Endgeräte mit schwachen Authentisierungsprotokollen nicht eingeschränkt, mit welchen Zielen und über welche Protokolle sie kommunizieren dürfen, können auch unberechtigte IT-Systeme, die durch einen der oben genannten Angriffe Zugang erhalten, weitreichende Kommunikationsmöglichkeiten erlangen.

2.4. Fehlerhafte Konfiguration der NAC-Lösung

Durch menschliche Fehler, unzureichende Prozesse oder unzureichende Personalkapazitäten und den dadurch bedingten Zeitmangel kann es passieren, dass die NAC-spezifischen Parameter an Endgeräten, Access-Switches oder RADIUS-Servern (NAC-Regelwerk) fehlerhaft konfiguriert werden. Dies kann dazu führen, dass sich die gesamte NAC-Lösung ungewollt falsch verhält, wodurch z. B. Endgeräte benötigte Ressourcen nicht erreichen können oder keinen Netzzugang erhalten.

Werden MAC-Adressen bewusst falsch registriert, können dadurch zu viele Ressourcen freigeschaltet werden, indem falsche Netzsegmente oder andere falsche Autorisierungsparameter zugewiesen werden.

2.5. Unzureichende Validierung von Konfigurationsänderungen

Unzureichende Änderungsprozesse, die Konfigurationsänderungen nicht oder nur unzureichend validieren, begünstigen Fehler in der Konfiguration. Hierdurch kann es passieren, dass für Endgeräte zu viel oder zu wenig schützenswerte Ressourcen erreichbar sind oder es ihnen gänzlich verwehrt wird, auf das Netz zuzugreifen. Wird z. B. NAC an Switch-Ports ohne zwingenden Grund abgeschaltet, können gegebenenfalls unberechtigte Endgeräte uneingeschränkt auf das Netz zugreifen. Wird neue Software auf Endgeräten unzureichend validiert, kann dies z. B. zu Interferenzen zwischen Software-Komponenten führen und die Funktionalität des Supplicants beeinflussen.

2.6. Unzureichend geschützter Netzzugang

Wird NAC an Switch-Ports temporär oder dauerhaft abgeschaltet, ist der Netzzugang unzureichend geschützt. Dadurch ist es möglich, dass unautorisierte Personen auf das Netz zugreifen können oder unsichere IT-Systeme zu weitgehende Kommunikationsberechtigungen erhalten. In der Folge kann unberechtigt auf Informationen zugegriffen und Informationen können manipuliert oder gelöscht werden. Außerdem kann auf diese Weise Schadsoftware eingeschleust werden.

Wird die Endgeräte-Compliance unzureichend geprüft, kann dies auch zu einem unzureichend geschützten Netzzugang führen, wenn das Endgerät z. B. über unzureichenden Virenschutz verfügt und dadurch Schadsoftware eingeschleust wird.

2.7. Ausfall oder unzureichende Erreichbarkeit der zentralen NAC-Komponenten

Ein unzureichendes oder unzureichend umgesetztes NAC-Konzept, gestörte NAC-Komponenten oder ein gestörtes Netz, unzureichende Anforderungsanalyse, mangelnde Prozesse oder Denial-of-Service-Angriffe (DoS-Angriffe) können dazu führen, dass die zentralen NAC-Komponenten ausfallen oder nicht erreichbar sind. Dies hat Auswir-

kungen auf die Fähigkeit der Endgeräte zu kommunizieren. Zum Beispiel haben, abhängig von der Switch-Konfiguration, Endgeräte bei Ausfall aller RADIUS-Server entweder keinen oder einen uneingeschränkten Netzzugang.

2.8. Nachverfolgung von Benutzenden

Ein unzureichendes Administrationskonzept, eine unzureichende Umsetzung der Konzeptionierung, zu lange Speicherzeiten oder eine mangelnde Abstimmung mit Betriebsrat und Datenschutzbeauftragten könnten dazu führen, dass personenrelevante Log-Daten unzureichend geschützt sind. Dadurch könnten Benutzendenprofile erstellt werden, die es ermöglichen, dass Mitarbeitende zeitlich nachverfolgt werden können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.3.4 *Network Access Control* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Institution

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.3.4.A1 Begründete Entscheidung für den Einsatz von NAC (B) [Institution]

Die Institution MUSS grundsätzlich entscheiden, ob und in welchem Umfang NAC eingesetzt wird. Die getroffene Entscheidung MUSS zusammen mit einer Begründung an geeigneter Stelle dokumentiert werden.

Wird NAC eingesetzt, MÜSSEN folgende Punkte geeignet thematisiert werden:

- Netzbereiche und Netzkomponenten, für die NAC realisiert werden soll
- Umgang mit internen Endgeräten und Fremdendgeräten
- Berücksichtigung von NAC bei der Beschaffung von neuen IT-Systemen

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.3.4.A2 Planung des Einsatzes von NAC (S)

Der Einsatz von NAC SOLLTE umfassend und detailliert geplant werden. Die Planung SOLLTE dabei mindestens folgende Aspekte beinhalten:

- Erstellung von Anforderungskatalogen für Endgeräte, Access-Switches und RADIUS-Server
- Prüfung und gegebenenfalls Ergänzung des IT-Asset-Managements
- Erstellung eines spezifischen NAC-Konzepts
- Festlegung von Beschaffungs-, Betriebs-, und Incident-Prozessen für NAC-Komponenten

- Migrationsplanung
- Monitoring und Logging der NAC-Lösung
- Anbindung an sicherheitsrelevante Komponenten (z. B. Firewalls, Virenschutz, Schwachstellen-Scanner, System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen)
- Zusatzfunktionen wie Profiling, Endgerätekonformitätsprüfung und Integritätsprüfung sowie Verschlüsselung auf Layer 2 mit MACsec

NET.3.4.A3 Erstellung eines Anforderungskatalogs für NAC (S)

Die Anforderungen an die NAC-Lösung SOLLTEN in einem Anforderungskatalog erhoben werden. Der Anforderungskatalog SOLLTE dabei die grundlegenden funktionalen Anforderungen umfassen und alle NAC-Komponenten (z. B. Endgeräte, Access-Switches und RADIUS-Server) adressieren.

Der Anforderungskatalog SOLLTE mit allen betroffenen Fachabteilungen, den zuständigen Gremien und den Richtlinien der Institution abgestimmt werden. Der Anforderungskatalog SOLLTE regelmäßig und bei Bedarf aktualisiert werden.

Wenn NAC-Komponenten beschafft werden, SOLLTEN zugehörige Anforderungen berücksichtigt werden.

Die NAC-Lösung SOLLTE auf Basis des Anforderungskatalogs getestet werden.

NET.3.4.A4 Erstellung eines NAC-Konzepts (S)

Ausgehend von der Entscheidung aus NET.3.4.A1 *Begründete Entscheidung für den Einsatz von NAC* und den Anforderungen an die NAC-Lösung SOLLTE ein NAC-Konzept erstellt werden. Das NAC-Konzept SOLLTE mit dem Segmentierungskonzept gemäß NET.1.1 *Netzarchitektur und –design* abgestimmt werden. Darüber hinaus SOLLTEN im NAC-Konzept mindestens folgende Aspekte festgelegt werden:

- Netzbereiche, in denen NAC eingeführt wird
- Authentisierung und Autorisierung
- Nutzung von Zusatzfunktionen
- Konfigurationsvorgaben für betroffene Endgerätetypen, Access-Switches und WLAN Access Points sowie WLAN Controller
- Aufbau der RADIUS-Infrastruktur und das grundlegende Regelwerk für NAC
- Anbindung an externe Sicherheitskomponenten wie Firewalls oder Virenschutz
- Anbindung an Verzeichnisdienste

Das NAC-Konzept SOLLTE alle technischen und organisatorischen Vorgaben beschreiben. Insbesondere SOLLTEN alle relevanten Prozesse und die Migration thematisiert werden.

Das NAC-Konzept SOLLTE regelmäßig geprüft und bei Bedarf aktualisiert werden.

NET.3.4.A5 Anpassung von Prozessen für Endgeräte bezüglich NAC (S)

Für die Endgeräte, die in die NAC-Lösung eingebunden werden, SOLLTE NAC in allen relevanten Prozessen angemessen berücksichtigt werden. Insbesondere SOLLTEN die Prozesse zu Inbetriebnahme, Austausch, Änderungen und Störungen angepasst werden.

Für Supplicant-Software, Konfiguration und Identitätsmerkmale (z. B. Zertifikate), die für NAC auf den Endgeräten erforderlich sind, SOLLTE ein Prozess festgelegt werden, um die Endgeräte zentral zu verwalten.

NET.3.4.A6 Festlegung von Notfallprozessen für NAC (S)

Wird die Wirkkette bei NAC gestört, SOLLTE erwogen werden, die Sicherheitsmechanismen von NAC temporär in angemessenem Umfang zu deaktivieren.

Bei den Notfallmaßnahmen, die im Notfallprozess festgelegt werden, SOLLTEN Produktivität und Informationssicherheit gegeneinander abgewogen werden. Dabei SOLLTEN die folgenden Optionen von Notfallmaßnahmen (RADIUS-down-Policies) betrachtet werden:

- Die bestehenden Verbindungen werden durch Mechanismen wie temporäre Aussetzung der Reauthentisierung beibehalten, jedoch werden alle neuen Anmeldeversuche abgelehnt, so dass das vorgesehene Sicherheitsniveau erhalten bleibt.
- Die dynamische Zuordnung wird für neue Anmeldeversuche ausgesetzt und stattdessen eine feste, vordefinierte Zuweisung von Netzsegmenten durch Access-Switches vorgenommen, so dass zumindest grundlegend kommuniziert werden kann.
- NAC wird auf den Access-Switches oder auf einzelnen Ports eines Access-Switches deaktiviert, so dass weiterhin uneingeschränkt kommuniziert werden kann.

RADIUS-down-Policies SOLLTEN mit den relevanten Sicherheitsrichtlinien der Institution abgestimmt werden.

NET.3.4.A7 Nutzung sicherer Authentisierungsverfahren (S)

Endgeräte SOLLTEN sichere Authentisierungsverfahren nach dem Stand der Technik verwenden. Endgeräte SOLLTEN automatisiert auf Basis von Zertifikaten oder Zugangskonten authentisiert werden.

Unsichere Authentisierungsverfahren SOLLTEN nur in begründeten Ausnahmefällen genutzt und die Entscheidung dokumentiert werden.

NET.3.4.A8 Festlegung der NAC-spezifischen Rollen und Berechtigungen für den RADIUS-Server (S)

Im Rollen- und Berechtigungskonzept für den RADIUS-Server SOLLTEN die verschiedenen Gruppen berücksichtigt werden, die wegen NAC auf einen RADIUS-Server zugreifen müssen, um diesen zu administrieren. Dies SOLLTE insbesondere dann sorgfältig geplant werden, wenn ein zentraler RADIUS-Server für die gesamte Institution bereitgestellt wird. Mindestens SOLLTEN die folgenden Gruppen mit NAC-spezifischem Zugriff auf den RADIUS-Server zusätzlich zum allgemeinen IT-Betrieb berücksichtigt werden:

- die jeweiligen Organisationseinheiten, die Access-Switches (RADIUS-Clients) für ihren Netzbereich administrieren
- die jeweiligen Zuständigen für Endgerätegruppen, die Identitäten (z. B. MAC-Adressen) ihrer entsprechenden Gruppen verwalten
- der First-Level-Support, der fehlerhafte RADIUS-Freigaben analysiert und gegebenenfalls die entsprechenden Freischaltungen anpasst

NET.3.4.A9 Festlegung eines angepassten NAC-Regelwerkes (S)

Für die NAC-Lösung SOLLTE ein NAC-Regelwerk definiert werden, das das NAC-Konzept umsetzt und festlegt, wie die Endgeräte auf das Netz zugreifen dürfen. Hierin SOLLTE für jedes Endgerät bzw. für jede Endgerätegruppe festgelegt werden, ob uneingeschränkt auf das Netz zugegriffen werden darf, ob der Zugriff verweigert wird oder ob nur Segmente mit eingeschränkten Kommunikationsmöglichkeiten erreichbar sind.

Im NAC-Regelwerk SOLLTE auch festgelegt werden, auf welcher Basis die Zugangskontrolle erfolgt. Hierfür SOLLTEN für alle Endgeräte die genutzten Authentisierungsmethoden und die Bedingungen für eine erfolgreiche Authentisierung festgelegt werden.

NET.3.4.A10 Sichere Nutzung von Identitäten (S)

Für die NAC-Authentisierung SOLLTEN individuelle Identitäten genutzt werden. Identitäten, die von mehr als einem Endgerät verwendet werden, SOLLTEN nur in begründeten Ausnahmefällen genutzt werden.

Alle Informationen, die für eine erfolgreiche Authentisierung benötigt werden, SOLLTEN nach aktuellem Stand der Technik vor unberechtigtem Zugriff abgesichert werden.

NET.3.4.A11 Sichere Konfiguration der NAC-Lösung (S)

Alle Komponenten der NAC-Lösung SOLLTEN sicher nach dem Stand der Technik konfiguriert werden. Hierfür SOLLTEN entsprechende Standard-Konfigurationen und Betriebshandbücher entwickelt und bereitgestellt werden.

Die vorgegebenen und umgesetzten Konfigurationen für die Komponenten der NAC-Lösung SOLLTEN regelmäßig überprüft und gegebenenfalls angepasst werden.

Auf Endgeräten SOLLTEN die Berechtigungen für die Benutzenden derart eingeschränkt werden, dass diese die Konfigurationsparameter für den Supplicant nicht manipulieren, den Supplicant nicht deaktivieren und die Schlüssel oder Passwörter für NAC nicht auslesen können.

Für Access-Switches oder für einzelne Ports von Access-Switches SOLLTE die NAC-Authentisierung nur in begründeten und zuvor festgelegten Ausnahmefällen deaktiviert werden. Hierfür SOLLTEN technische Maßnahmen genutzt werden, die gegebenenfalls durch organisatorische Maßnahmen ergänzt werden.

NET.3.4.A12 Monitoring der NAC-Lösung (S)

Die zentralen RADIUS-Server und alle Access-Switches mit Authenticator sowie alle weiteren zentralen Dienste, die für die NAC-Lösung essentiell sind, SOLLTEN in ein möglichst umfassendes und einheitliches Monitoring eingebunden werden. Ergänzend zum allgemeinen Monitoring gemäß OPS.1.1.1 *Allgemeiner IT-Betrieb* SOLLTEN alle NAC-spezifischen Parameter überwacht werden, die die Funktionalität der NAC-Lösung oder der entsprechenden Dienste sicherstellen.

Insbesondere SOLLTE die Verfügbarkeit des RADIUS-Protokolls überprüft werden. Hierfür SOLLTEN RADIUS-Anfragen an aktive Konten erzeugt werden, um die gesamte NAC-Wirkkette inklusive der externen Verzeichnisdienste zu prüfen.

Für die Access-Switches SOLLTE der Status von NAC in das Monitoring einbezogen werden, um ein Deaktivieren von NAC zu erkennen.

Abweichungen von definierten Zuständen und Grenzwerten SOLLTEN dem IT-Betrieb gemeldet werden.

NET.3.4.A13 Erstellung von Validierungsvorgaben für die NAC-Konfiguration (S)

Für die NAC-Lösung SOLLTEN Validierungsvorgaben erstellt werden, um sicherzustellen, dass die NAC-Komponenten das NAC-Konzept angemessen umsetzen. Die Validierungsvorgaben SOLLTEN insbesondere die unterschiedlichen Funktionsdetails für die verschiedenen NAC-Komponenten berücksichtigen.

Die Validierung SOLLTE als Soll-Ist-Vergleich regelmäßig sowie bei Bedarf für die zentralen NAC-Komponenten und die Access-Switches durchgeführt werden.

NET.3.4.A14 Umsetzung weiterer Maßnahmen bei Verwendung von MAC-Adress-Authentisierung (S)

Endgeräte, die nicht über eine sichere EAP-Methode authentisiert werden können und anhand ihrer MAC-Adresse identifiziert werden, SOLLTEN NICHT als vertrauenswürdige Endgeräte eingestuft werden. Der Netzzugang SOLLTE auf das notwendige Minimum beschränkt werden.

Hierfür SOLLTEN weitere Maßnahmen wie Nutzung von Kommunikationsbeschränkungen oder nachgelagertes Endgeräte-Profiling der Endgeräte-Aktivitäten umgesetzt werden.

NET.3.4.A15 Anbindung Virenschutz an NAC-Lösung (S)

Jedes Endgerät SOLLTE auf Schadsoftware geprüft werden, bevor es an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift. Hierfür SOLLTE für die NAC-Endgeräte ein geeigneter Virenschutz mit der NAC-Authentisierung und -Autorisierung gekoppelt werden.

Falls das Virenschutzprogramm Schadsoftware meldet, SOLLTE die NAC-Lösung mit geeigneten Maßnahmen reagieren.

NET.3.4.A16 Protokollierung der Ereignisse (S)

Ergänzend zu OPS.1.1.5 *Protokollierung* SOLLTEN Statusänderungen an NAC-Komponenten sowie alle relevanten NAC-spezifischen, gegebenenfalls sicherheitskritischen Ereignisse protokolliert werden. Zusätzlich SOLLTEN alle schreibenden Konfigurationszugriffe auf die zentralen NAC-Komponenten protokolliert werden.

Es SOLLTE festgelegt werden, welche Protokollierungsdaten mit welchen Details erfasst und welche Daten auf einer zentralen Protokollierungsinstanz zusammengeführt werden.

Protokollierungsdaten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

Sicherheitskritische Ereignisse wie RADIUS-down oder eine ungewöhnliche Anzahl von RADIUS-Anfragen SOLLTEN zu einem automatischen Alarm führen.

NET.3.4.A17 Positionierung des RADIUS-Servers im Management-Bereich (S)

Der RADIUS-Server SOLLTE in einem geschützten Netzsegment innerhalb des Management-Bereichs (siehe NET.1.1 *Netzarchitektur und -design*) positioniert werden. Kommunikationsanfragen an den RADIUS-Server SOLLTEN nur von vertrauenswürdigen Quellen zugelassen werden. Diese SOLLTEN auf ein Minimum eingeschränkt werden.

Der RADIUS-Server SOLLTE NICHT direkt mit Endgeräten kommunizieren, sondern ausschließlich über den Authenticator auf den Access-Switches. Anfragen der Access-Switches SOLLTEN nur aus dem gemeinsamen Management-Netzsegment akzeptiert werden.

NET.3.4.A18 Dokumentation der NAC-Lösung (S)

Die NAC-Lösung mit allen NAC-Komponenten SOLLTE geeignet dokumentiert werden.

Aus der Dokumentation SOLLTE mindestens hervorgehen, auf welchen Komponenten und Endgeräten NAC mit welchen Parametern genutzt wird und welche Abhängigkeiten zwischen den Komponenten existieren. Auch SOLLTE das Regelwerk für Authentisierung und Autorisierung, das in Software-Code vorliegt, ergänzend in vereinfachter, verständlicher Form dokumentiert werden. Darüber hinaus SOLLTE die Konfiguration aller NAC-Komponenten, gegebenenfalls kategorisiert, umfassend dokumentiert werden.

Die Dokumentation SOLLTE bei jeder Änderung fortgeschrieben und stets aktuell gehalten werden. Die Aktualität der Dokumentation SOLLTE regelmäßig und bei Bedarf geprüft werden.

NET.3.4.A19 Ordnungsgemäße Verwaltung von Identitäten zur Authentisierung (S)

Alle Identitäten, die via NAC einen Zugang zum Netz der Institution ermöglichen, SOLLTEN geeignet geschützt und verwaltet werden. Hierzu SOLLTEN mindestens die folgenden Punkte festgelegt werden:

- Handhabung und Schutz von Zertifikaten
- Prüfen, Sperren und Löschen von nicht mehr genutzten Identitäten
- Prozess und Schnittstellen zur Sperrung einer Identität

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

NET.3.4.A20 Einsatz von MACsec (H)

Für jedes Datenpaket SOLLTE die Datenintegrität gewährleistet werden. Darüber hinaus SOLLTE erwogen werden, diese Daten zu verschlüsseln. Hierfür SOLLTE MACsec gemäß IEEE 802.1AE genutzt werden.

Access-Switches und Endgeräte, die MACsec nicht unterstützen oder für die MACsec nicht eingerichtet werden soll, SOLLTEN erfasst werden. Für diese SOLLTE regelmäßig überprüft werden, ob die Ausschlussgründe noch gelten.

NET.3.4.A21 Einsatz von Endgerätekonformitätsprüfung (H)

Bevor ein Endgerät an das Netz der Institution angebunden wird und bevor es auf IT-Systeme der Institution zugreift, SOLLTE geprüft werden, ob es den Konformitätsvorgaben der Institution genügt (Compliance Check).

Für jedes Endgerät SOLLTE festgelegt werden, welche Vorgaben das Endgerät einzuhalten hat. Endgeräte, die nicht den Konformitätsvorgaben der Institution genügen, SOLLTEN nur stark eingeschränkt auf das Netz der Institution zugreifen dürfen.

Die NAC-Lösung SOLLTE mit einem Werkzeug zur Konformitätsprüfung verbunden werden, das eine Bewertung des Zustands der Endgeräte vornimmt und an die NAC-Lösung meldet. Auf dieser Basis SOLLTE die NAC-Lösung steuern, wie die Endgeräte auf das Netz zugreifen dürfen.

NET.3.4.A22 NAC-Autorisierung mit Mikrosegmenten (H)

Endgeräte mit ähnlichem Anforderungsprofil und identischem Schutzbedarf SOLLTEN via NAC getrennten Netzsegmenten zugewiesen werden.

Darüber hinaus SOLLTE erwogen werden, ob mit NAC eine Mikrosegmentierung der zu autorisierenden Endgeräte umgesetzt wird.

NET.3.4.A23 Einsatz von autarken RADIUS-Servern für unterschiedliche Netzbereiche und Funktionen (H)

Für NAC SOLLTEN dedizierte und autarke RADIUS-Server eingesetzt werden. Weitere Funktionen wie VPN-Zugriffsregelung SOLLTEN NICHT gemeinsam mit NAC-Funktionen auf einem gemeinsamen RADIUS-Server realisiert werden.

Zusätzlich SOLLTE erwogen werden, dedizierte und autarke RADIUS-Server für unterschiedliche Netze bereitzustellen. Hier SOLLTEN insbesondere getrennte RADIUS-Server erwogen werden, um Office- und Produktions-Endgeräte oder LAN- und WLAN-Endgeräte getrennt abzusichern.

Darüber hinaus SOLLTE erwogen werden, für einzelne Netz- oder Funktionsbereiche eigenständige RADIUS-Server einzurichten.

NET.3.4.A24 Nutzung sicherer Protokolle zwischen NAC-Komponenten (H)

Für die Kommunikation zwischen den zentralen NAC-Komponenten SOLLTEN grundsätzlich Protokolle verwendet werden, die nach dem Stand der Technik als sicher gelten. Für die Kommunikation zwischen dem RADIUS-Server und einem gegebenenfalls genutzten Verzeichnisdienst SOLLTEN nur sichere Protokolle eingesetzt werden.

Darüber hinaus SOLLTE auch geprüft werden, ob für die Kommunikation zwischen dem RADIUS-Server und Access-Switches sichere Protokolle eingesetzt werden sollen.

NET.3.4.A25 Einbindung der NAC-Lösung in ein Sicherheitsmonitoring (H)

Die NAC-Lösung SOLLTE in ein Sicherheitsmonitoring eingebunden werden. Dies SOLLTE zumindest für die zentralen NAC-Komponenten und für die weiteren zentralen Dienste, die von der NAC-Lösung genutzt werden, umgesetzt werden.

NAC-spezifische Sicherheitsereignisse (z. B. häufige Zurückweisung von Anfragen oder die Mehrfachverwendung von Identitäten) SOLLTEN in eine Alarmierung übernommen werden.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen NAC-Komponenten sowie gegebenenfalls die weiteren zentralen Dienste hierin eingebunden werden.

NET.3.4.A26 Hochverfügbarkeit der zentralen NAC-Komponenten (H)

Die zentralen NAC-Komponenten SOLLTEN redundant ausgelegt werden. Alle weiteren zentralen Dienste, die für die Funktionsfähigkeit der NAC-Lösung essentiell sind, SOLLTEN auch hochverfügbar ausgelegt sein.

Die für die Hochverfügbarkeit relevanten Parameter SOLLTEN in Monitoring und Protokollierung integriert werden. Statusänderungen und Warnmeldungen SOLLTEN regelmäßig kontrolliert und gegebenenfalls in eine Alarmierung einbezogen werden.

Die RADIUS-down-Policies, mit denen eine Kommunikation auch bei ausgefallenem RADIUS-Dienst gewährleistet wird, SOLLTEN das Sicherheitsniveau des Netzes NICHT senken.

NET.3.4.A27 Prüfung der Notwendigkeit für MAC-Adress-Authentisierung (H)

Eine Authentisierung über MAC-Adressen SOLLTE nur dort genutzt werden, wo dies technisch unumgänglich ist und die Sicherheitsrichtlinien dies zulassen.

Es SOLLTE im Vorfeld geprüft werden, ob solche Ausnahmefälle notwendig sind. Ist dies der Fall, SOLLTEN die Ausnahmefälle auf den minimalen Einsatzbereich eingeschränkt werden.

Die Begründung und das Ergebnis der Prüfung SOLLTEN dokumentiert werden. Sie SOLLTEN regelmäßig und bei Bedarf nochmals verifiziert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein NET.3.4 *Network Access Control* sind keine weiterführenden Informationen vorhanden.

Bundesamt
für Sicherheit in der
Informationstechnik

NET.4.1 TK-Anlagen

1. Beschreibung

1.1. Einleitung

Mit einer Telekommunikationsanlage, kurz TK-Anlage, können die Telefone einer Institution intern verbunden und extern an ein öffentliches Telefonnetz angeschlossen werden. Durch die zunehmende Verzahnung von IT und Telekommunikation können TK-Anlagen dabei sowohl analog als auch IP-basiert aufgebaut sein. Hybrid-Anlagen sind eine Kombination aus einer klassischen Telekommunikationslösung und einem VoIP-System. Mit einer Hybrid-Anlage können klassische digitale und analoge Telefonie sowie VoIP gleichzeitig betrieben werden.

Neben der Sprachtelefonie können, abhängig von den angeschlossenen Endgeräten, weitere Dienste genutzt werden. So ist es möglich, mittels TK-Anlagen Daten, Texte, Grafiken und Bewegtbilder zu übertragen. Die Informationen können dabei analog oder digital über drahtgebundene oder drahtlose Übertragungsmedien weitergeleitet werden. Je nach Anbindung und genutzten Datennetzen können in einer Institution verschiedenste Telekommunikationsanlagen eingesetzt werden.

1.2. Zielsetzung

In diesem Baustein werden die für die TK-Anlagen sowie die entsprechenden Anteile von Hybrid-Anlagen spezifischen Gefährdungen und Anforderungen betrachtet. Das Ziel des Bausteins ist der Schutz der Informationen, die über TK-Anlagen übermittelt werden sowie der Schutz der Anlage vor Fremdeingriffen und Manipulationen.

1.3. Abgrenzung und Modellierung

Der Baustein NET.4.1 *TK-Anlagen* ist auf jede TK-Anlage anzuwenden.

Dieser Baustein behandelt die Gefährdungen und Anforderungen, die spezifisch für eine TK-Anlage sowie die entsprechenden Teile einer Hybrid-Anlage sind. Themen, die über die TK-Anlage hinausgehen, wie zum Beispiel Gefährdungen und Anforderungen für einzelne VoIP-Implementierungen, sowie extern bereitgestellte Dienste werden in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums gesondert behandelt.

Die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP werden im Baustein NET.4.2 *VoIP* näher betrachtet.

TK-Anlagen sollten grundsätzlich mit berücksichtigt werden, wenn die Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.2.5 *Fernwartung*, CON.3 *Datensicherungskonzept* und OPS.1.1.5 *Protokollierung* umgesetzt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein NET.4.1 *TK-Anlagen* von besonderer Bedeutung.

2.1. Abhören von TK-Anlagen

Wenn Telefongespräche oder Daten über eine TK-Anlage unverschlüsselt übertragen werden, besteht grundsätzlich die Gefahr, dass Angreifende Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmenden vermittelnden TK-Anlage lauschen.

Bei vielen TK-Anlagen können Anrufende Empfangenden Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von Angreifenden abgefangen und angehört werden.

Des Weiteren könnten Gespräche durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen, Leistungsmerkmalen von Dritten mitgehört werden. Ein Beispiel hierfür ist die Zeugenschaltung. Eine derartige Aktivierung erfordert zwar genauere Systemkenntnisse, ist aber aufgrund vieler frei verfügbarer Hinweise im Internet häufig kein großes Hindernis.

2.2. Abhören von Räumen über TK-Anlagen

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei werden zwei Varianten unterschieden:

Bei der ersten Variante können Endgeräte, wenn entsprechende Funktionen implementiert sind, aus dem öffentlichen Netz oder über das LAN dazu veranlasst werden, die eingebauten Mikrofone zu aktivieren. Ein bekanntes Beispiel hierfür ist die sogenannte „Baby-Watch-Funktion" von Telefonen oder Anrufbeantwortern.

Bei der zweiten Variante kann das Leistungsmerkmal „direktes Ansprechen" in Kombination mit der Option „Freisprechen" missbraucht werden. Die auf diese Weise realisierbare Funktion einer Wechselsprechanlage kann unter gewissen Umständen auch zum Abhören eines Raumes ausgenutzt werden.

2.3. Gebührenbetrug

Gebührenbetrug im Zusammenhang mit Daten- oder Telekommunikationsdiensten hat das Ziel, die Kosten für geführte Telefonate oder Datentransfers auf Dritte zu übertragen. Eine TK-Anlage lässt sich auf verschiedene Weise von außen manipulieren. Zum einen können Angreifende versuchen, vorhandene Leistungsmerkmale für den Gebührenbetrug zu missbrauchen. Zu diesen Leistungsmerkmalen zählen beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-in-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende „Amtsleitungen" abgehende „Amtsleitungen" belegen. Auf diese Weise können Anrufenden bei Anwahl einer bestimmten Rufnummer auf Kosten des TK-Anlagenbetreibenden von außen automatisch wieder mit dem „Amt" verbunden werden.

Darüber hinaus können nicht nur Angreifende von außen, sondern auch die Beschäftigten innerhalb einer Institution mit den Gebühren betrügen. So können sie etwa versuchen, auf Kosten der Institution oder der anderen Beschäftigten zu telefonieren, indem sie z. B. von fremden Apparaten telefonieren, fremde Berechtigungscodes (Passwörter) auslesen oder persönliche Berechtigungen verändern.

2.4. Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinen Benutzenden persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besuchende frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystemen. Besitzen diese Telefone ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins NET.4.1 *TK-Anlagen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Fachverantwortliche
Weitere Zuständigkeiten	IT-Betrieb, Vorgesetzte

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

NET.4.1.A1 Anforderungsanalyse und Planung für TK-Anlagen (B) [IT-Betrieb]

Vor der Beschaffung oder Erweiterung einer TK-Anlage MUSS eine Anforderungsanalyse durchgeführt werden. Im Rahmen dieser Analyse MUSS festgelegt werden, welche Funktionen die TK-Anlage bieten soll. Hierbei MÜSSEN neben der Ausprägung der TK-Anlage auch die Anzahl der benötigten Verbindungen und Anschlüsse festgelegt werden. Auch eine mögliche Erweiterbarkeit und grundlegenden Sicherheitsfunktionen MÜSSEN bei der Planung betrachtet werden. Darüber hinaus MÜSSEN je nach Bedarf Support- und Wartungsverträge für die TK-Anlage berücksichtigt werden. Basierend auf den ermittelten Anforderungen MUSS anschließend der Einsatz der TK-Anlage geplant und dokumentiert werden. Die zuvor ermittelten Anforderungen und die Planung MÜSSEN mit den entsprechenden IT-Zuständigen abgestimmt werden.

NET.4.1.A2 Auswahl von TK-Diensteanbietenden (B) [IT-Betrieb]

Um mit Personen telefonieren zu können, deren Telefone nicht an die institutionseigene TK-Anlage angeschlossen sind, MUSS ein TK-Diensteanbieter oder eine TK-Diensteanbieterin beauftragt werden. Dabei MÜSSEN die Anforderungen an die TK-Anlage, die Sicherheitsrichtlinie sowie vertragliche und finanzielle Aspekte berücksichtigt werden. Alle vereinbarten Leistungen MÜSSEN eindeutig schriftlich festgehalten werden.

NET.4.1.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.1.A5 Protokollierung bei TK-Anlagen (B)

Bei TK-Anlagen MÜSSEN geeignete Daten erfasst und bei Bedarf ausgewertet werden. Protokolliert werden MÜSSEN zusätzlich alle systemtechnischen Eingriffe, die Programmveränderungen beinhalten, sowie Auswertungsläufe, Datenübermittlungen und Datenzugriffe. Alle Administrationsarbeiten an der TK-Anlage MÜSSEN ebenfalls protokolliert werden. Die protokollierten Informationen SOLLTEN regelmäßig kontrolliert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.4.1.A6 Erstellung einer Sicherheitsrichtlinie für TK-Anlagen (S) [IT-Betrieb]

Basierend auf der institutionsweiten Sicherheitsrichtlinie SOLLTE eine eigene Sicherheitsrichtlinie für die TK-Anlage erstellt werden. Diese Sicherheitsrichtlinie für die TK-Anlage SOLLTE grundlegende Aussagen zur Vertraulichkeit, Verfügbarkeit und Integrität beinhalten. Sie SOLLTE allen Personen, die an der Beschaffung, dem Aufbau, der Umsetzung und dem Betrieb der TK-Anlage beteiligt sind, bekannt sein und die Grundlage für deren Arbeit darstellen. Die zentralen sicherheitstechnischen Anforderungen an die TK-Anlage sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweite Sicherheitsrichtlinie aufgenommen werden.

NET.4.1.A7 Geeignete Aufstellung der TK-Anlage (S)

Die TK-Anlage SOLLTE in einem geeigneten Raum untergebracht sein. Die Schnittstellen an der TK-Anlage, besonders nicht genutzte Schnittstellen, SOLLTEN geeignet geschützt werden.

NET.4.1.A8 Einschränkung und Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale (S)

Der Umfang der verfügbaren Leistungsmerkmale SOLLTE auf das notwendige Minimum beschränkt werden. Nur die benötigten Leistungsmerkmale SOLLTEN freigeschaltet werden. Die nicht benötigten oder wegen ihres Missbrauchspotenzials als kritisch eingestuften Leistungsmerkmale SOLLTEN so weit wie möglich an der zentralen Anlage abgeschaltet werden. Zusätzliche Schutzmaßnahmen SOLLTEN für die auf den Endgeräten gespeicherten und abrufbaren vertraulichen Daten ergriffen werden.

NET.4.1.A9 Schulung zur sicheren Nutzung von TK-Anlagen (S) [Vorgesetzte]

Die Benutzenden der TK-Anlage SOLLTEN in die korrekte Verwendung von Diensten und Geräten eingewiesen werden. Den Benutzenden der TK-Anlage SOLLTEN alle notwendigen Unterlagen zur Bedienung der entsprechenden Endgeräte zur Verfügung gestellt werden. Sämtliche Auffälligkeiten und Unregelmäßigkeiten der TK-Anlage SOLLTEN den entsprechenden Verantwortlichen gemeldet werden.

NET.4.1.A10 Dokumentation und Revision der TK-Anlagenkonfiguration (S) [IT-Betrieb]

Die TK-Anlagenkonfiguration SOLLTE geeignet dokumentiert und fortgeschrieben werden. Die TK-Anlagenkonfiguration SOLLTE in regelmäßigen Abständen überprüft werden. Das Ergebnis der Prüfung SOLLTE zumindest den Informationssicherheitsbeauftragten, den Fachverantwortlichen und anderen verantwortlichen Mitarbeitenden vorgelegt werden.

NET.4.1.A11 Außerbetriebnahme von TK-Anlagen und -geräten (S) [IT-Betrieb]

Die Aussonderung von TK-Anlagen und angeschlossenen TK-Geräten SOLLTE in der Sicherheitsrichtlinie berücksichtigt werden. Alle Daten, die auf TK-Anlagen oder Endgeräten gespeichert sind, SOLLTEN vor der Aussonderung sicher gelöscht werden.

NET.4.1.A12 Datensicherung der Konfigurationsdateien (S)

Die Konfigurations- und Anwendungsdaten der eingesetzten TK-Anlage SOLLTEN bei der Ersteinrichtung und anschließend regelmäßig gesichert werden, insbesondere nachdem sich diese geändert haben. Es SOLLTE regelmäßig geprüft und dokumentiert werden, ob die Sicherungen der TK-Anlagen auch tatsächlich als Basis für eine Systemwiederherstellung genutzt werden können.

Es SOLLTE ein Datensicherungskonzept für TK-Anlagen erstellt und mit den allgemeinen Konzepten der Datensicherung für Server und Netzkomponenten abgestimmt werden.

NET.4.1.A13 Beschaffung von TK-Anlagen (S)

Bei der Beschaffung von TK-Anlagen SOLLTEN die Ergebnisse der Anforderungsanalyse und der Planung miteinbezogen werden. Bei der Beschaffung einer TK-Anlage SOLLTE beachtet werden, dass sie neben digitalen auch analoge Teilnehmeranschlüsse anbieten sollte. Darüber hinaus SOLLTEN vorhandene Kommunikationssysteme und -komponenten bei der Beschaffung berücksichtigt werden.

NET.4.1.A14 Notfallvorsorge für TK-Anlagen (S)

Es SOLLTE ein Notfallplan für die TK-Anlage erstellt werden. Dieser SOLLTE in das Notfallkonzept der Institution integriert werden. Es SOLLTEN regelmäßig Notfallübungen bezüglich der TK-Anlagen durchgeführt werden.

NET.4.1.A15 Notrufe bei einem Ausfall der TK-Anlage (S)

Es SOLLTE sichergestellt werden, dass auch bei einem Ausfall der TK-Anlage Notrufe aus der Institution abgesetzt werden können. Die Notrufmöglichkeiten SOLLTEN von allen Räumen aus auf ausreichend kurzen Wegen erreichbar sein.